HP Designjet Printer series

Security features

© 2014 Hewlett-Packard Development Company, L.P.

Reproduction, adaptation, or translation without prior permission is prohibited, except as allowed under the copyright laws.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

July Edition
Version 6

Table of Contents

1. Introduction & Overview 4
2. Security features available for Large Format Printers 4
3. Security features available for Large Format scanners 9
4. Security Concepts explanation 10
3.1 Secure File Erase 10
3.2 Secure Disk Erase 11
3.3 Control Panel Access Lock 14
3.3.1 Deadlock: Front Panel locked + EWS password forgotten 15
3.4 Embedded Web Server (EWS) multilevel access 16
3.4.1 Administrator password 16
3.4.2 Guest password 18
3.5 Exclude personal info from accounting 20
3.6 Disable connectivity interfaces 21
3.7 Disable protocols 22
3.8 IPSec 22
3.9 SNMPv3 23
3.10 CA/JD Certificates 24
3.11 Hide IP from front panel 24
3.12 Encrypt web communications 24
3.13 Disable USB drive 25
3.14 Disable firmware update through USB 25
3.15 Disable direct print using ePrint&Share 25
3.16 Disable ePrint Center connectivity 26
3.17 User sessions 26
3.18 Disable internet connection 26
3.19 Printer Access control 26
3.20 External hard disk (EHD) 26
3.21 Jetdirect Security Wizard (HP T920-T1500-T2500-T3500) 27
3.22 Job storage and PIN printing 28
3.23 Self Encrypted hard disk 29
5. Other security features available only through JetDirect 30
4.1 Access Control list 30
4.2 802.1X Authentication 30
6. Glossary 31

1. Introduction & Overview

This document provides an overview of the security features supported by HP Designjet printers as of January 2014.

The security features described in this document make the HP Designjet printer series particularly well suited for deployment in environments where network, data, and access control security are important.

The following is a table summarizing the new and existing security features of HP Designjet printers series and how they are implemented using the Embedded Web Server and/or HP Web JetAdmin (WJA). Please make sure that your printer has the latest firmware version to benefit from all security features.

Note: If your printer is not listed in the table then these features are not implemented.

2. Security features available for Large Format Printers

	Z6X00	D 5800	Z5400	Z3200	Z2100/Z5200ps
Hide information to user					
Control panel lock	EWS	EWS	EWS/WJA	N/A	N/A
Hide IP from Front Panel (FP)	FP	FP	EWS/FP	N/A	N/A
EWS multilevel	EWS	EWS	FP	EWS (1 level)	N/A
Printer access control	N/A	N/A	EWS/FP	N/A	N/A
Exclude personal info. from accounting	EWS	EWS	EWS	EWS	EWS (Z5200ps only)
Job Storage Mode and PIN printing	N/A	N/A	N/A	N/A	N/A
Disable features					
Disable USB drive	N/A	N/A	EWS/FP	N/A	N/A
Disable firmware (F/W) update thru USB	N/A	N/A	EWS/FP	N/A	N/A
Disable interfaces	EWS	EWS	EWS/FP (USB printing only)	N/A	N/A
Disable internet connection	N/A	N/A	FP	N/A	N/A
Disable ePrint Center connectivity	N/A	N/A	EWS/FP	N/A	N/A
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Wizard setup configuration	N/A	N/A	N/A	N/A	N/A

Data access					
Secure file erase	WJA	WJA	WJA	WJA	WJA (Z2100 only)
Secure disk erase	WJA/FP	WJA/FP	WJA/FP	WJA/FP	N/A
External HDD	YES	YES	N/A	N/A	N/A
Self-Encrypted hard disk	N/A	N/A	N/A	N/A	N/A
Communications security					
IPSec	EWS	EWS	EWS/WJA	EWS/WJA + JetDirect	EWS/WJA + JetDirect
Wizard setup configuration	N/A	N/A	N/A	N/A	N/A
SNMPv3	EWS	EWS	EWS	EWS/WJA + JetDirect	EWS/WJA + JetDirect
CA/JD Certificates	EWS/WJA	EWS/WJA	EWS/WJA	EWS + JetDirect	EWS + JetDirect
Encrypt web comms	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA + JetDirect	EWS/WJA + Jetdirect
NTLM	N/A	N/A	N/A	N/A	N/A

	T7X00	T3500	T2500/T1500/T920	T2300/T1300	T790	T120/T520
Hide information to user						
Control panel lock	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	N/A
EWS multilevel	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS / FP (1 level)	EWS (1 level)
Hide IP from FP	FP	FP	FP	FP	FP	N/A
Printer access control	N/A	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS/FP	N/A
Exclude personal info. from accounting	EWS	EWS/WJA	EWS/WJA	EWS	EWS	N/A
Job storage and PIN printing (Job retention)	N/A	YES	N/A	N/A	N/A	N/A
Disable features						
Disable USB drive	N/A	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS/FP	N/A
Disable F/W update thru USB	N/A	EWS/FP	EWS/FP	EWS/FP	EWS/FP	N/A
Disable interfaces	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS/FP (USB printing only)	EWS / FP (USB printing only)	EWS/FP
Disable ePrint Center connectivity	N/A	EWS/FP	EWS/FP	FP	FP	EWS/FP
Disable internet connection	N/A	EWS/FP/WJA	EWS/FP/WJA	EWS/FP	EWS/FP	EWS/FP
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Data access						
Secure file erase	WJA	EWS/FP/WJA	EWS/FP/WJA	WJA	WJA	N/A
Secure disk erase	WJA/FP	EWS/FP/WJA	EWS/FP/WJA	WJA/FP	WJA/FP (PS models)	N/A
External HDD	Yes	N/A	N/A	Yes	PS only	N/A
Self-Encrypted hard disk	N/A	Yes	N/A	N/A	N/A	N/A

Communications security						
Wizard setup configuration	N/A	EWS	EWS	N/A	N/A	N/A
IPSec	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS/WJA	EWS/WJA	requires Jetdirect accessory
SNMPv3	EWS	EWS/FP/WJA	EWS/FP/WJA	EWS	EWS	N/A
CA/JD Certificates	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS	N/A
Encrypt web comms	EWS/WJA	EWS/FP/WJA	EWS/FP/WJA	EWS/WJA	EWS/WJA	EWS
NTLM	N/A	V2 and V1	V1	V1	N/A	N/A

	T1200	T770	Z3100	Z3100ps	4020/4520	T1100/ T1120	Z6100	T620
Hide information to user								
Control panel lock	EWS/WJA	WJA	N/A	N/A	WJA	EWS	EWS	N/A
EWS multilevel	EWS	N/A	N/A	EWS (1 level)	EWS	EWS	EWS	N/A
Hide IP from FP	FP	FP	N/A	N/A	FP	FP	FP	N/A
Printer access control	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Exclude personal info. from accounting	EWS	EWS	N/A	N/A	EWS	EWS	EWS	N/A
Disable features								
Disable USB drive	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable F/W update thru USB	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable interfaces	EWS	EWS	EWS	N/A	EWS	EWS	EWS	N/A
Disable ePrint Center connectivity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable internet connection	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Disable protocols	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA	EWS/WJA
Data access								
Secure file erase	WJA	WJA	WJA	WJA	WJA	WJA	WJA	N/A
Secure disk erase	WJA/FP	WJA/FP (HD)	N/A	FP	FP	WJA/FP	WJA/FP	WJA/FP
External HDD	Yes	HD ver (from F/W 6.0.0.6)	N/A	N/A	N/A	N/A	N/A	N/A
Self-Encrypted hard disk	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Communications security								
IPSec	EWS/WJA	EWS/WJA	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect
Wizard setup configuration	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
SNMPv3	EWS	EWS	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS+ Jetdirect	EWS + Jetdirect	EWS + Jetdirect
CA/JD Certificates	EWS	EWS	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect	EWS + Jetdirect
Encrypt web comms	EWS	EWS	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect	EWS/WJA + Jetdirect
NTLM	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

3. Security features available for Large Format scanners

Multi-function printers (MFPs) consist of two main parts: the printer and the scanner. For the printer, the table above applies. For the scanner, refer to the table below:

	HP Designjet HD Pro Scanner	**DJ 4500MFP/T1100MFP HD-MFP Series DJ4520 Scanner, DJ 4500 Scanner, HD Scanner**	**T1120 SD-MFP**	**T2300 eMFP**	**T2500 eMFP**
Firewall	Yes	Yes	Yes	Yes	Yes
Antivirus installation	Closed systems with very low risk of being infected by a virus, so no antivirus is required				
Disable FTP & WebAccess	Yes	Yes	N/A	Yes	Yes
Access to images in scanner through network	Yes, by default (FTP & EWS - Read only)	Yes, by default (FTP & EWS - Read only)	N/A	N/A	N/A
Microsoft Security patches	Yes through scanner S/W update			Not needed (Linux based)	Not needed (Linux based)
Install scanner software into a separate PC	N/A	Possible but not official process	N/A	N/A	N/A

4. Security Concepts explanation

3.1 Secure File Erase

Secure File Erase is a feature that manages how files are deleted from the printer's hard disk.

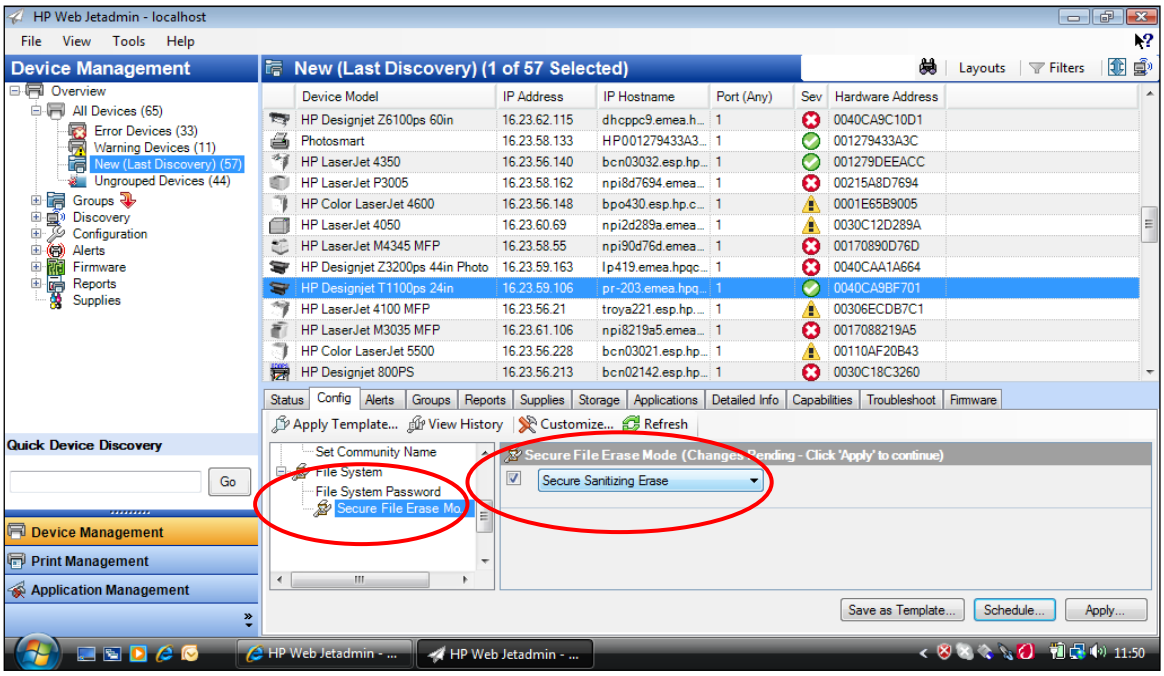
There are three security modes to the Secure Files Erase feature. These settings can be changed via Web JetAdmin.

- *Non-Secure Fast Erase*: In this mode, all file pointers to the data (table indexes) are erased. Temporary data remains on the Hard Disk Drive until the disk space it occupies is needed for another purpose, and is then overwritten. This is the fastest mode of operation and is the default for all printers.
- *Secure Fast Erase*: In this mode of operation, file pointers are erased and the disk space where the temporary job was stored is also overwritten with a fixed character pattern. This mode of operation is slower than Non-Secure Fast Erase, but all data is overwritten.
- *Secure Sanitizing Erase*: In this mode of operation, file pointers are erased and the disk space where the temporary job was stored is repeatedly overwritten using an algorithm that prevents any residual data. This mode of operation may affect product performance. The Secure Sanitizing Erase mode of operation meets the US Department of Defense 5220.22-M requirements for clearing and sanitization of disk media. When the Secure Sanitizing Erase feature is enabled, all temporary files that might contain sensitive data are erased with this method. No temporary files are left after a job has been completed (scan, copy, or print).

Furthermore, if you do not want to store jobs in the printer, you can set the number of jobs to be stored in the printer's queue to 0. To configure this setting perform the following steps:

- Go to the printer's front panel,
- Select the "setup" menu.
- Select "job management setup."

For further information, refer to the printer's user manual, as the actual menu options may differ for a specific printer. The following is an example of how to change the 'Secure File Erase' setting for the HP Designjet T1100 printer.

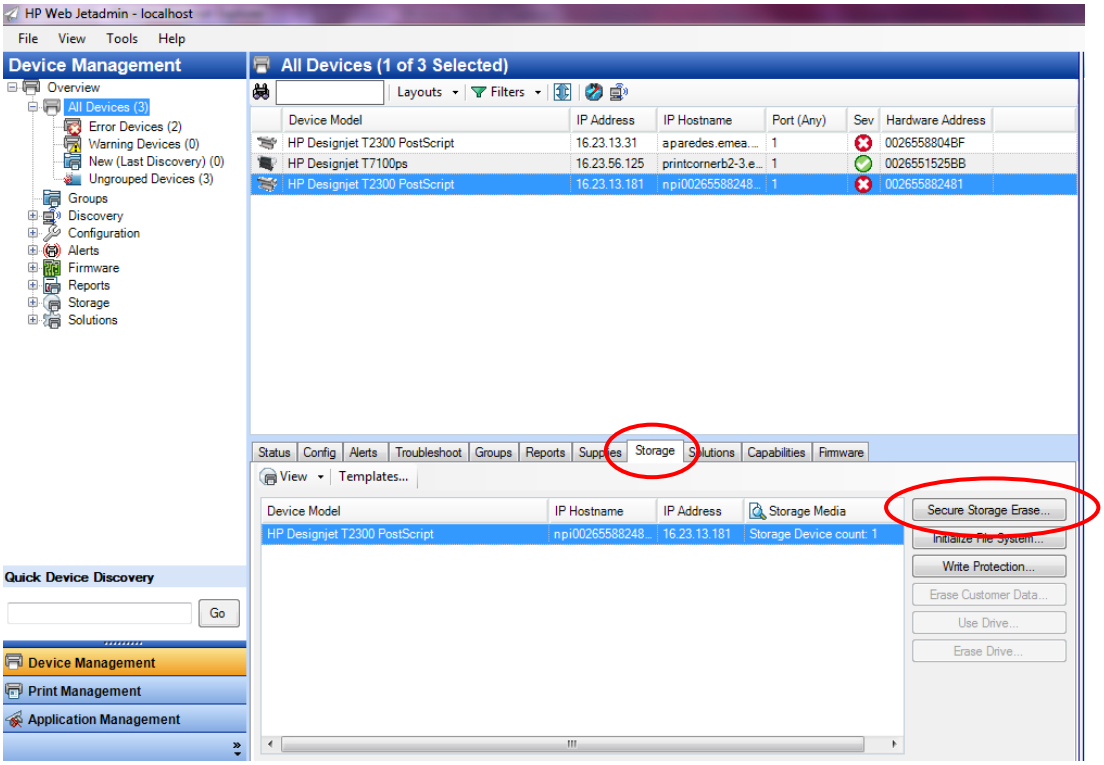


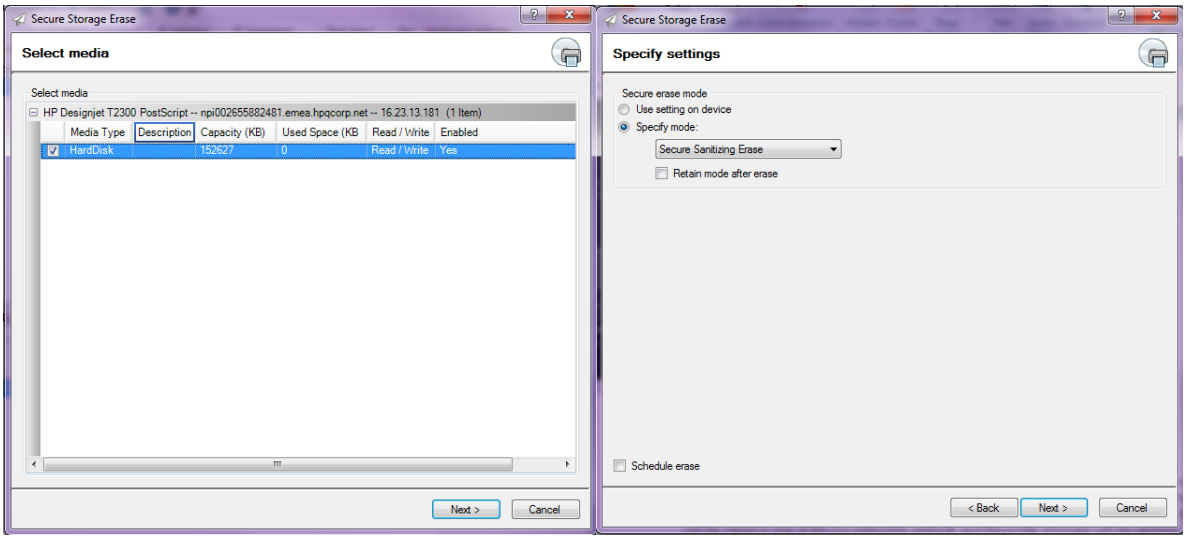
3.2 Secure Disk Erase

In either of the two secure methods described above (Secure Fast Erase and Secure Sanitizing Erase), there is also the option to sanitize the whole disk. The sanitizing method removes any user data in a secure manner, so that the device can safely be moved from a secure location to an unsecure location. All disk erasing will be carried out via the same level of security erase.

This setting can only be used via Web JetAdmin or the Front Panel “Service menu”, which is only accessible with the help of an HP Support representative.

- **HP Web JetAdmin access**: The user interface that manages the Secure File Erase and Secure Disk Erase functionality is the HP Web JetAdmin. This is the same functionality that is used in the Web JetAdmin device plug-ins for LaserJet printers, which enables you to set the same global options across your fleet of HP LaserJets and HP Designjets. The following example shows how to configure the HP Designjet T2300 using the Web JetAdmin. Note that in the Web JetAdmin this option is called “Secure Storage Erase”.

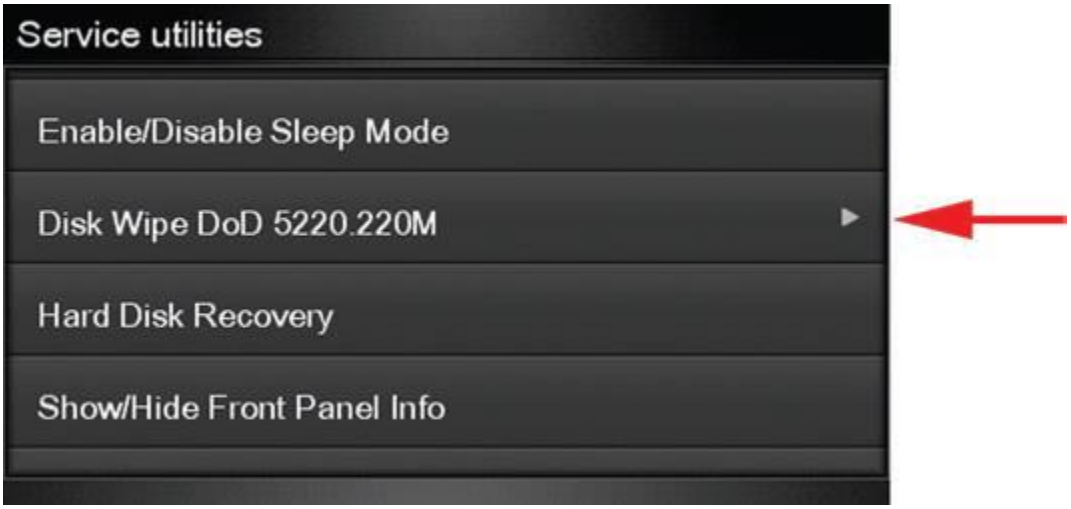


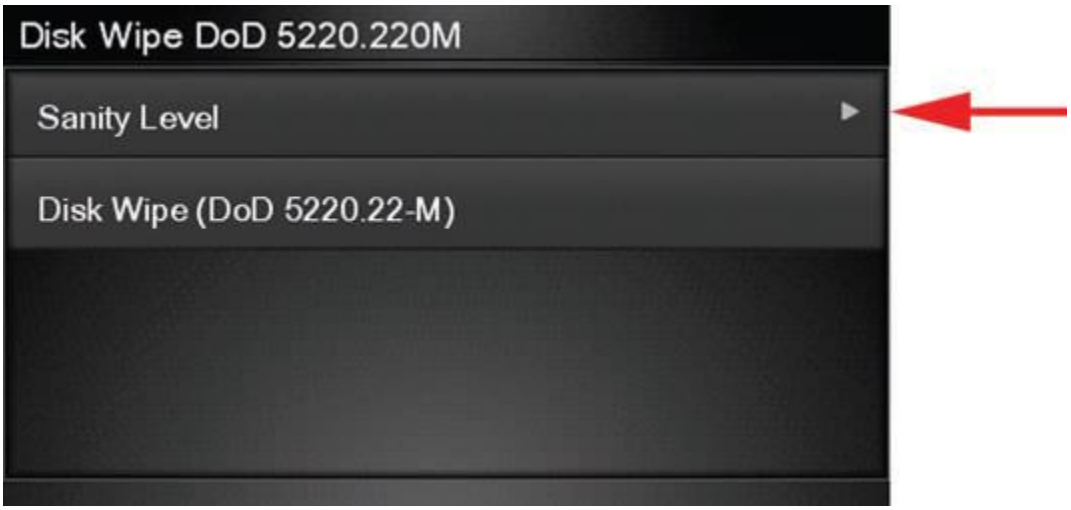


- **Printer Front Panel access:** Once you have entered into the "Service Menu" with the help of an HP Support representative, you can perform the Secure Disk Erase using the same 3 options that you have in Web JetAdmin. Note that the name of the feature in the front panel is **Disk Wipe DoD 5220.220M**, and the three options are called "Insecure Mode", "1-pass mode" and "5-pass mode".

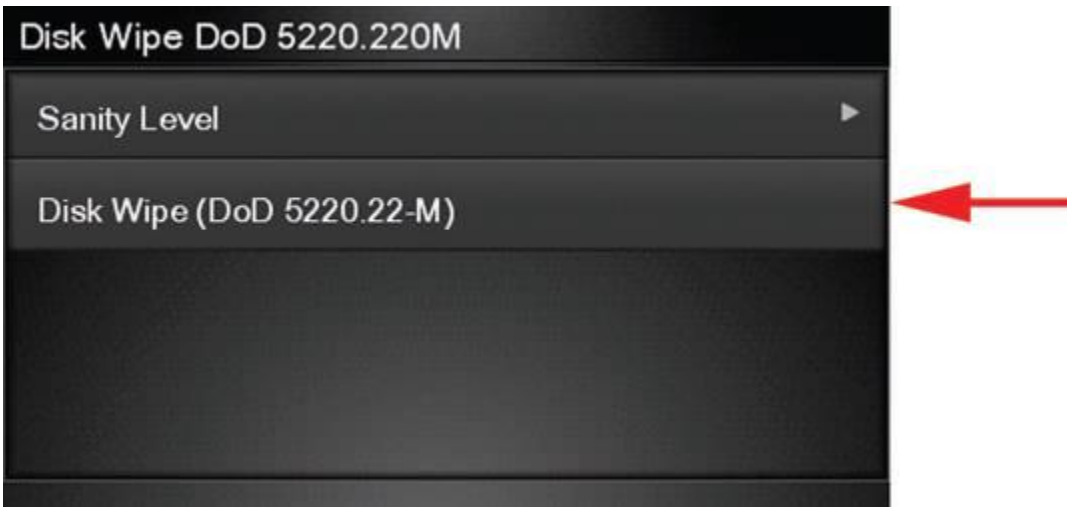
Before you start the erase operation, you must first select the security level (sometimes referred to as sanity level). The printer will then warn you that the erase operation is a process which deletes all data and takes a long time. Once you accept, the printer will begin the process, and displays a progress bar until complete. All data will be wiped using the selected method, and the printer's firmware will be restored to the latest version installed before this operation.

The following screens show how to perform a secure hard disk erase on the HP Designjet T2300 printer.





Sanity Level
Insecure Mode
1-Pass Mode
5-Pass Mode

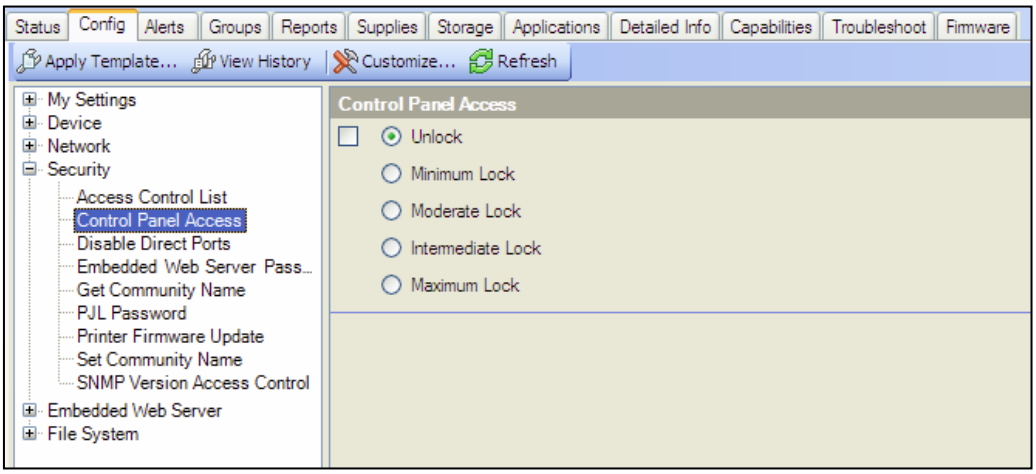

Disk Wipe DoD 5220.220M
Sanity Level
Disk Wipe (DoD 5220.22-M)

3.3 Control Panel Access Lock

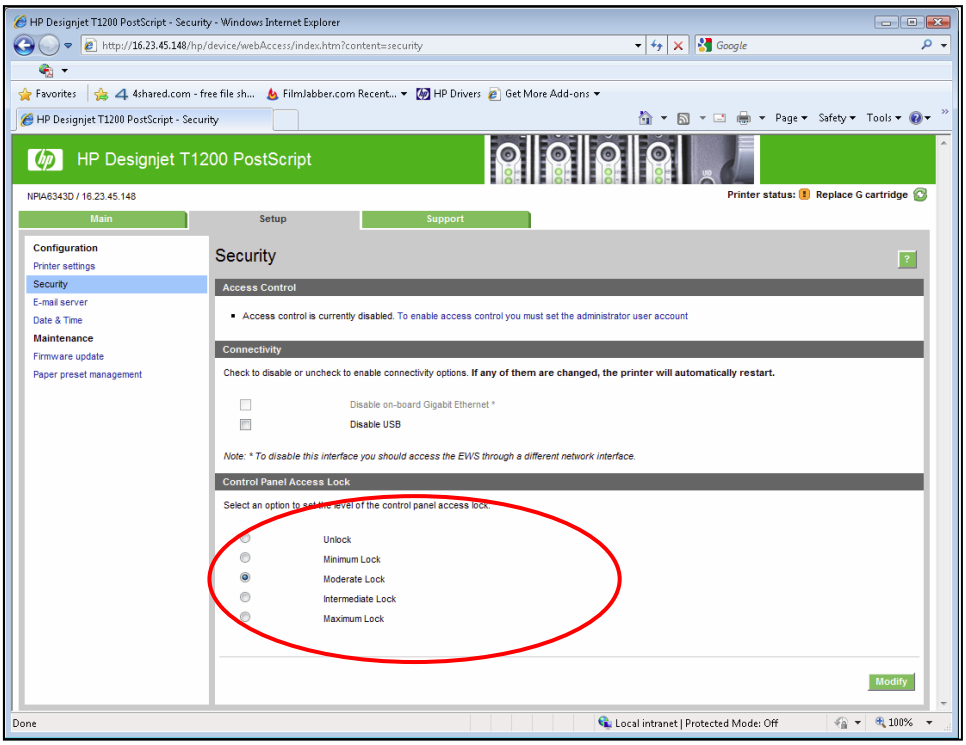
The control panel access lock is a feature intended for IT administrators, which enables them to lock the device's control panel by using either the HP Web JetAdmin or the printer's Embedded Web Server (depending on the printer model). This feature prevents unauthorized users from accessing the control panel and changing the printer's settings. Administrators can specify the level of access as follows:

- Unlock
- Minimum lock
- Moderate lock
- Intermediate lock
- Maximum lock

This option can be enabled from the HP Web JetAdmin as shown below:



This option can be enabled from the T1200 Embedded Web server as shown below:



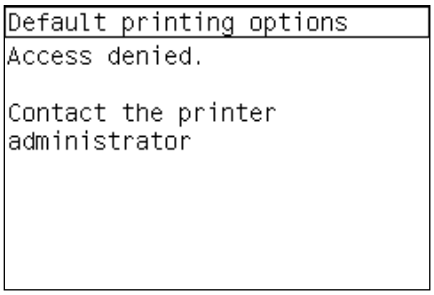
The following table shows the different levels of access and what they enable or disable:

	Retrieve Job	Information	Paper handling	Configure Designjet	Diagnostics
Maximum	OK	----	----	----	----
Intermediate	OK	OK	----	----	----
Moderate	OK	OK	OK	----	----
Minimum	OK	OK	OK	OK	OK

- **Maximum Lock** – This option denies access to all options.
- **Intermediate Lock** – This option denies access to the paper and ink supply handling options, maintenance options and demo prints as well as the options locked by Moderate Lock. Only viewing printer and supply information is allowed.
- **Moderate Lock** – This option denies access to all printer settings, the job queue, information and service prints and the printer log, as well as the options locked by Minimum Lock. For ePrinters, the setting also locks access to these 5 security features:
    - Disable USB drive
    - Disable firmware update through USB
    - Disable direct print using ePrint&Share
    - Disable ePrint connectivity
    - Disable internet connection
- **Minimum Lock** – This option denies access to the Reset options, Enable/Disable connectivity options and the Service Menu.

Note: When the Moderate or Maximum locks are set, you will not able to load/unload paper or replace printheads/ink cartridges without first unlocking the front panel, and so these options should only be set in specific circumstances where the implications are known and understood.

When the Control Panel is locked, the applicable menus show a 'lock' symbol in the front panel. If a user attempts to access a "locked" menu entry, a warning message is displayed.



3.3.1 Deadlock: Front Panel locked + EWS password forgotten

Under certain circumstances, a printer might become inaccessible if the control panel has been locked and the administrator has lost the password needed to unlock it. This could happen if the front panel is locked through the printer's Embedded Web Server and the Administrative password for the EWS is lost. In this situation, it would not be possible to unlock the front panel from the Embedded Web Server and it would not be possible to reset the Embedded Web Server from the front panel.

With HP Designjet Printers there is a menu option that users can access with the guidance of Customer Support agents. If you encounter any problems related to deadlock, then you should contact HP Support as soon as possible.

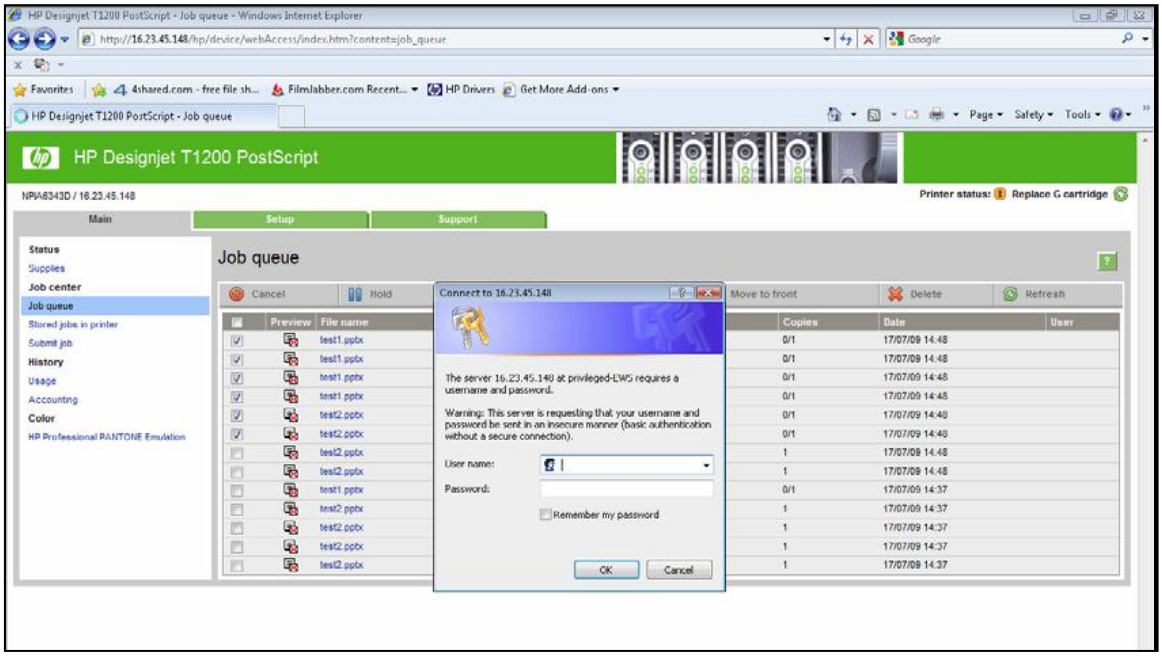
3.4 Embedded Web Server (EWS) multilevel access

The Embedded Web Server is a powerful tool which enables direct management of a device such as an HP LaserJet printer or an HP Designjet printer. With no security in place, however, this tool also has the potential to have a negative effect on many features, as they can be configured using just a web browser and knowledge of the IP address of to the printer. To solve this situation we have implemented two levels of access to our compatible HP Designjet printers.

The Security page enables users to:

- Restrict access to the printer by setting an administrator user account.
- Define two levels of access: Administrator and Guest.

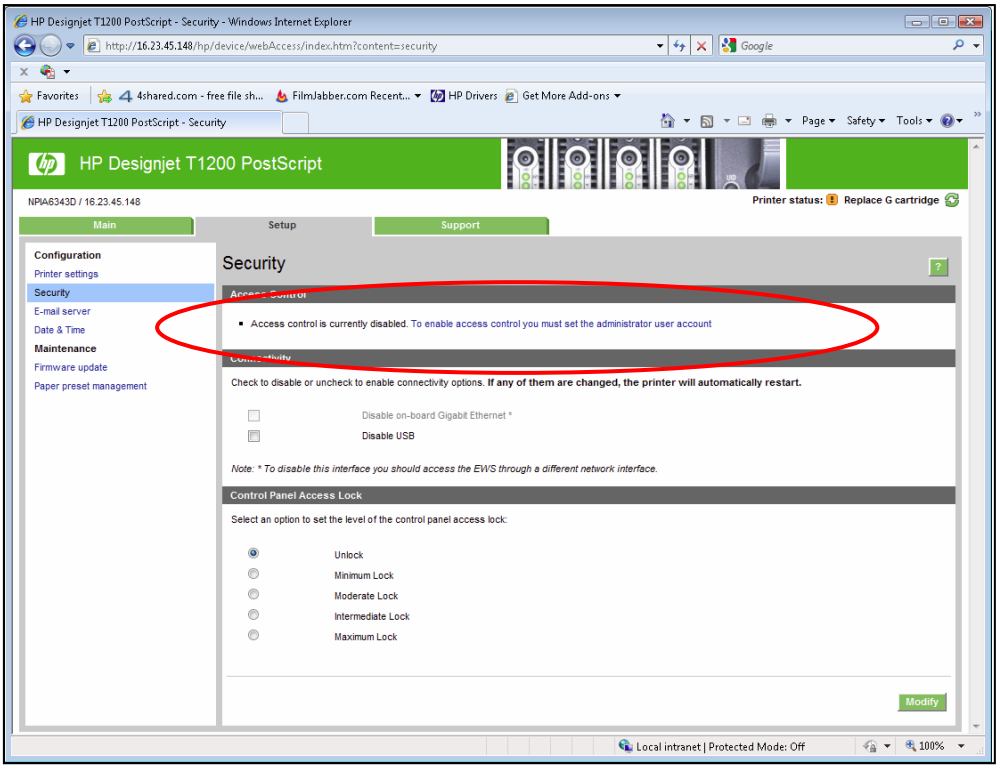
If the two levels of access have been set, and you have neither of the passwords, then you will not be able to gain access to EWS information, as in the image below.

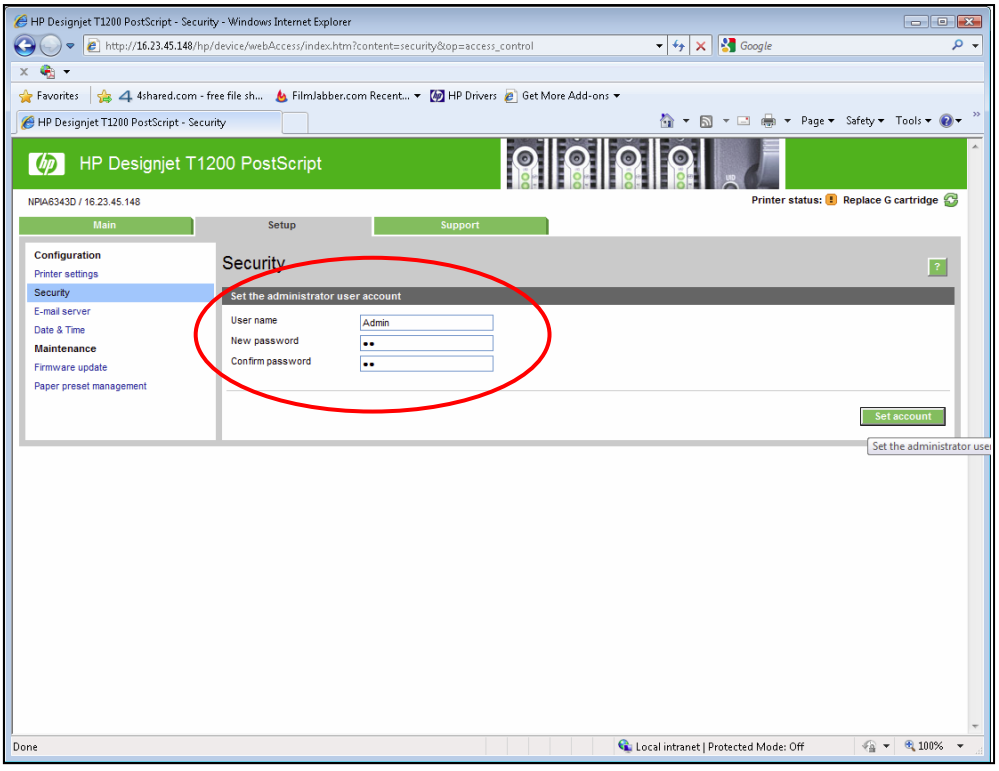


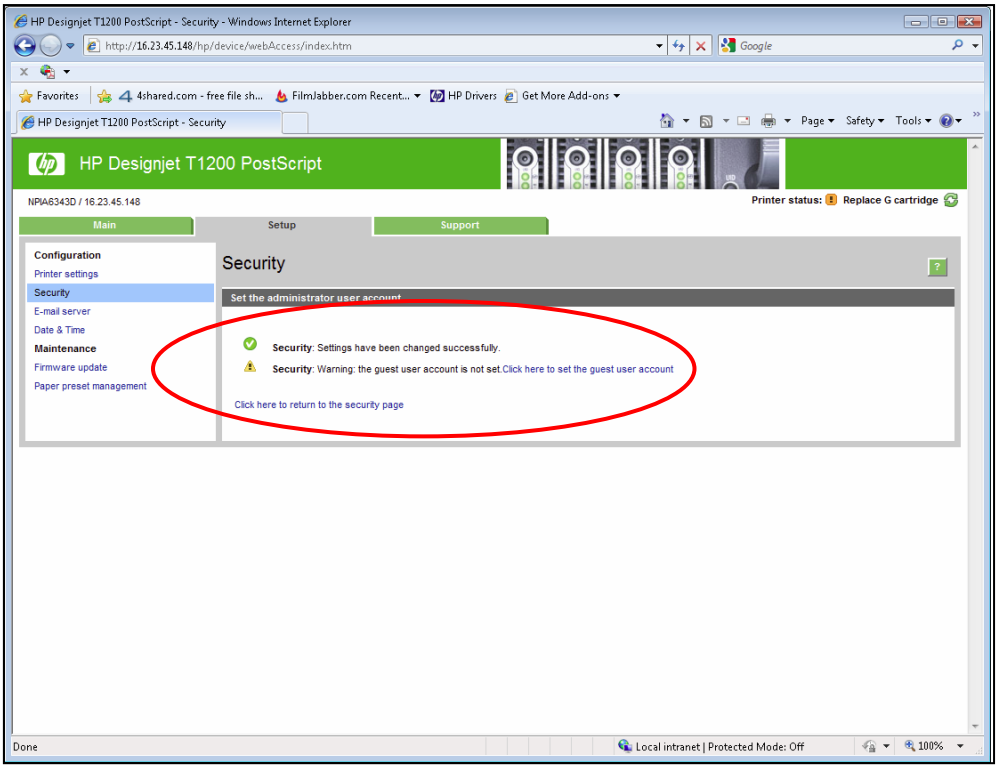
3.4.1 Administrator password

Access control is enabled by setting the “Admin account password”, i.e. specifying a password for the user account at Admin level. You must then provide the Admin password in order to perform any of the following restricted operations:

- Cancel, delete or preview a job in the job queue.
- Delete a stored job.
- Clear accounting information.
- Change printer settings on the Device Setup page.
- Update printer firmware.
- Change the printer's date and time.
- Change security settings.
- View protected printer information pages.


HP Designjet T1200 PostScript - Security - Windows Internet Explorer
http://16.23.45.148/hp/device/webAccess/index.htm?content=security
HP Designjet T1200 PostScript
NPIA6343D / 16.23.45.148
Printer status: Replace G cartridge
Main
Setup
Support
Configuration
Printer settings
Security
E-mail server
Date & Time
Maintenance
Firmware update
Paper preset management
Security
Access control is currently disabled. To enable access control you must set the administrator user account
Check to disable or uncheck to enable connectivity options. If any of them are changed, the printer will automatically restart.
Disable on-board Gigabit Ethernet *
Disable USB
Note: * To disable this interface you should access the EWS through a different network interface.
Control Panel Access Lock
Select an option to set the level of the control panel access lock:
Unlock
Minimum Lock
Moderate Lock
Intermediate Lock
Maximum Lock
Modify


HP Designjet T1200 PostScript - Security - Windows Internet Explorer
http://16.23.45.148/hp/device/webAccess/index.htm?content=security&op=access_control
HP Designjet T1200 PostScript
NPIA6343D / 16.23.45.148
Printer status: Replace G cartridge
Main
Setup
Support
Configuration
Printer settings
Security
E-mail server
Date & Time
Maintenance
Firmware update
Paper preset management
Security
Set the administrator user account
User name
Admin
New password
Confirm password
Set account



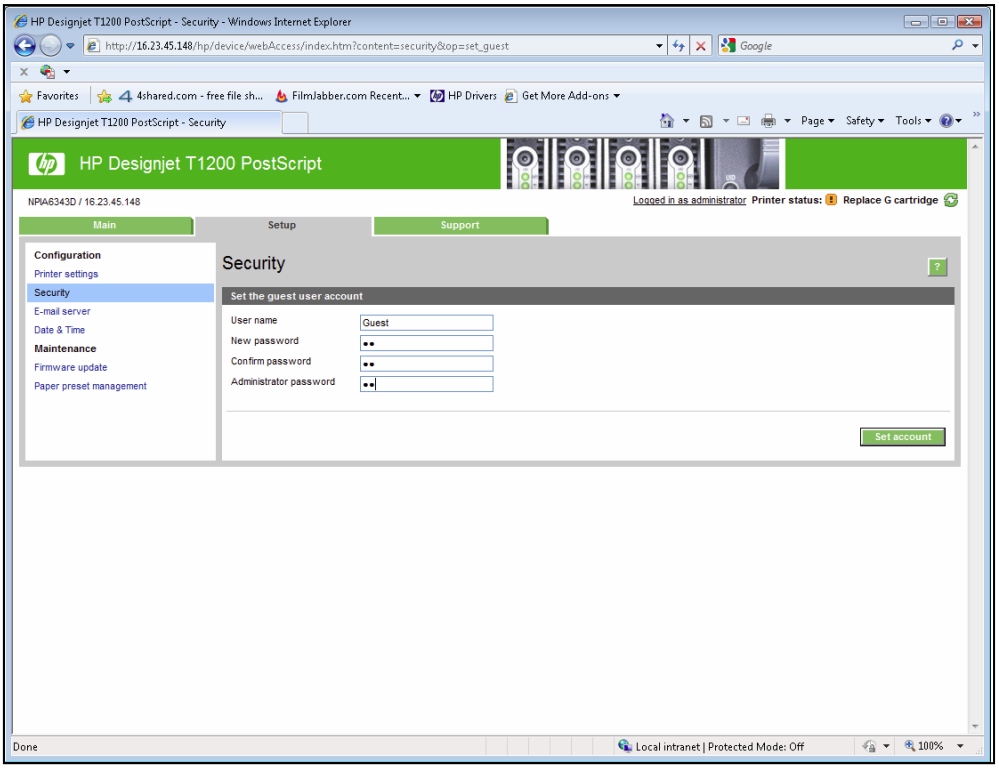
If there is no administrator account, then the restricted operations can be accessed without a password.

3.4.2 Guest password

Once the administrator user account has been set, the administrator can also set up a guest user account by specifying a password for the guest.

If the guest user account is set up, a username and password are required for **all** EWS operations: users identified as guests have access to restricted operations, whilst users identified as administrators have access to all operations.

If the guest account is not set up, a username and password are not required for unrestricted operations.



Notes:

- Some printers only have 1-level password access to the Embedded Web Server.
- The networking tab of the Embedded Web Server enables you to set up another password. If the printer has a EWS 1-level or multi-level password, then the networking password is the same as the general EWS password. If the EWS does not have password capabilities, then the networking password is only used for controlling access to the networking area of the EWS.
- For most printers that have EWS password capability, it is also possible to setup the Admin password through Web JetAdmin. Only one level can be set in this way, however, so the Guest password cannot be set up from Web JetAdmin.
- Passwords have no minimum complexity requirements, so the minimum password length is 1 character.
- Eprinters with touch screen front panels only allow the use of the limited set of characters shown below (capital letters are also supported).

```
q w e r t y u i o p
a s d f g h j k l _
z x c v b n m @ .

1 2 3 4 5 6 7 8 9 0
, - # ; : " + = * '
! ? < > \ / ( ) @ .

¡ ¿ € £ $ % & ~ [ ]
ñ à á â è é â ê ì í î
ò ó ô ù ú û Ç @ .
```

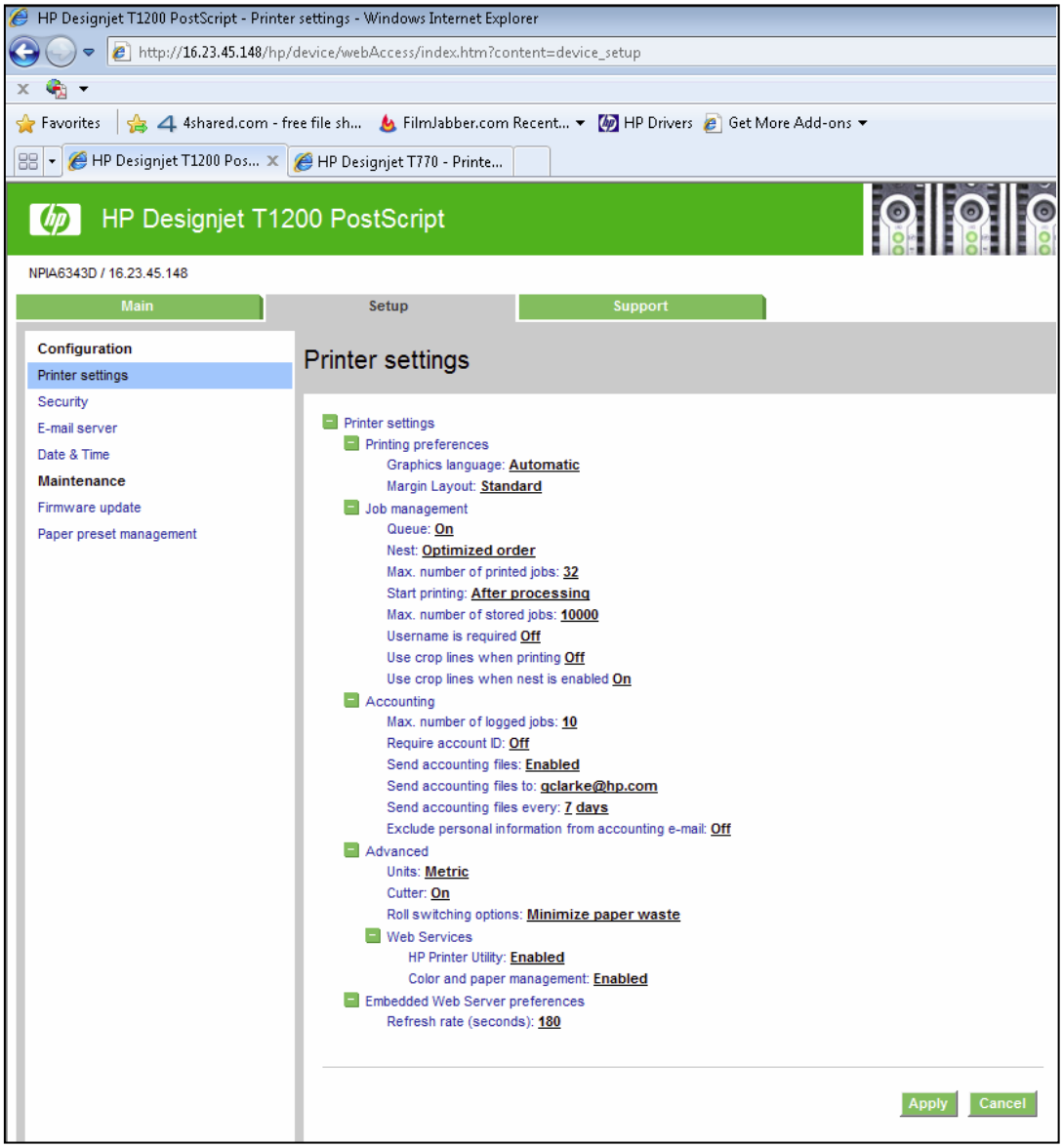
- These limitations do not apply to printers without touch screen front panels, as the password can be set using EWS.
- Some printer drivers rely on the EWS for creating the preview. In cases where an administrator password is set, the administrator password will be required to access job preview.

3.5 Exclude personal info from accounting

You can enable or disable the option for the printer to send an e-mail containing accounting information. If you enable this setting, you also need to fill in the destination of the report by using the “Send accounting files to” setting. Please note that you also have to configure the e-mail server on the **Setup Page**.

In some cases, customers prefer not to send personal data from the printers via e-mail, and so the option to Exclude Personal information from accounting e-mail is now available in the Embedded Web server. If this option is selected, accounting e-mails will not contain personal information (user name, job name, and account ID will be left blank in the accounting file sent by e-mail from the printer).

This option is typically used for managed print or pay-per-use contracts in order to ensure that only the data (counters) relevant for billing are being sent by the printer. Personal information about who printed which file is not required for billing purposes, and can be excluded from the accounting e-mail. This personal information is typically used for cost allocation within a company.

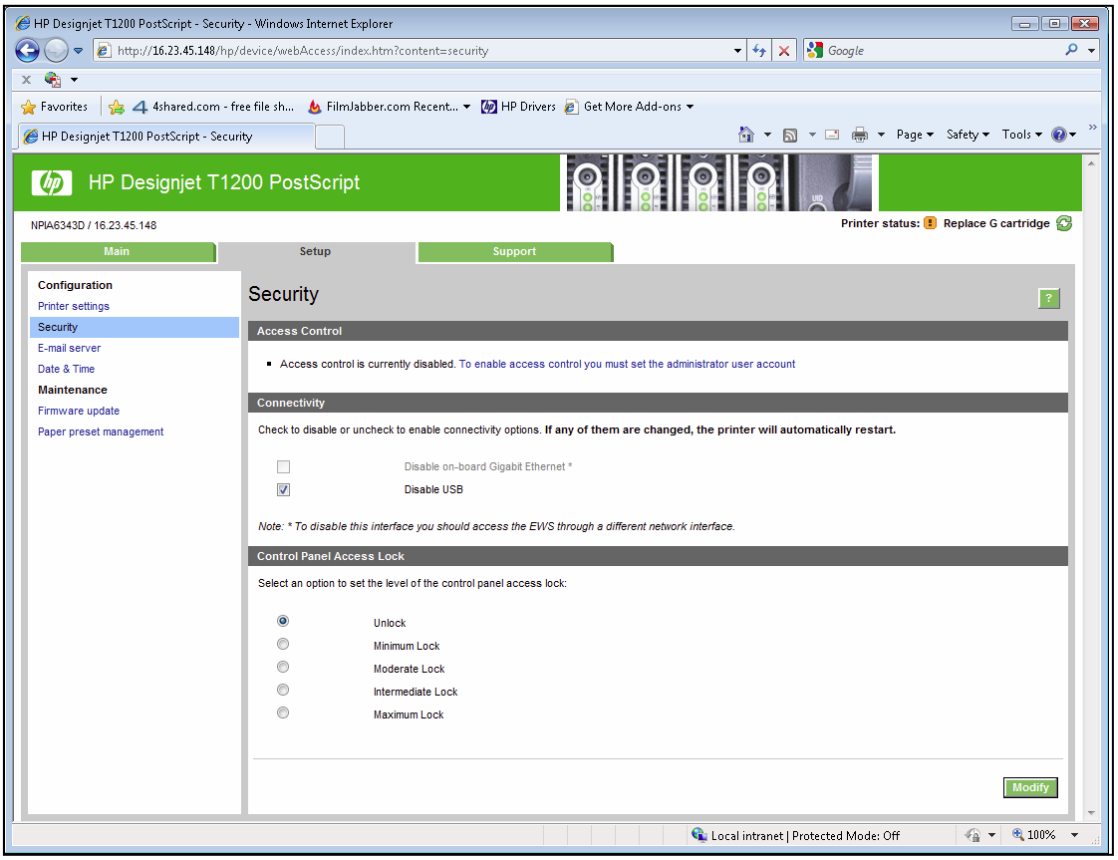


3.6 Disable connectivity interfaces

Depending on the printer series, there are some ports that can be disabled to prevent unauthorized printing and possible data theft.

You might want to disable the USB printing port to prevent people from connecting a laptop directly into the printer and printing via USB.

If you have installed a JetDirect card to add extra security features, you might want to disable the onboard Ethernet.

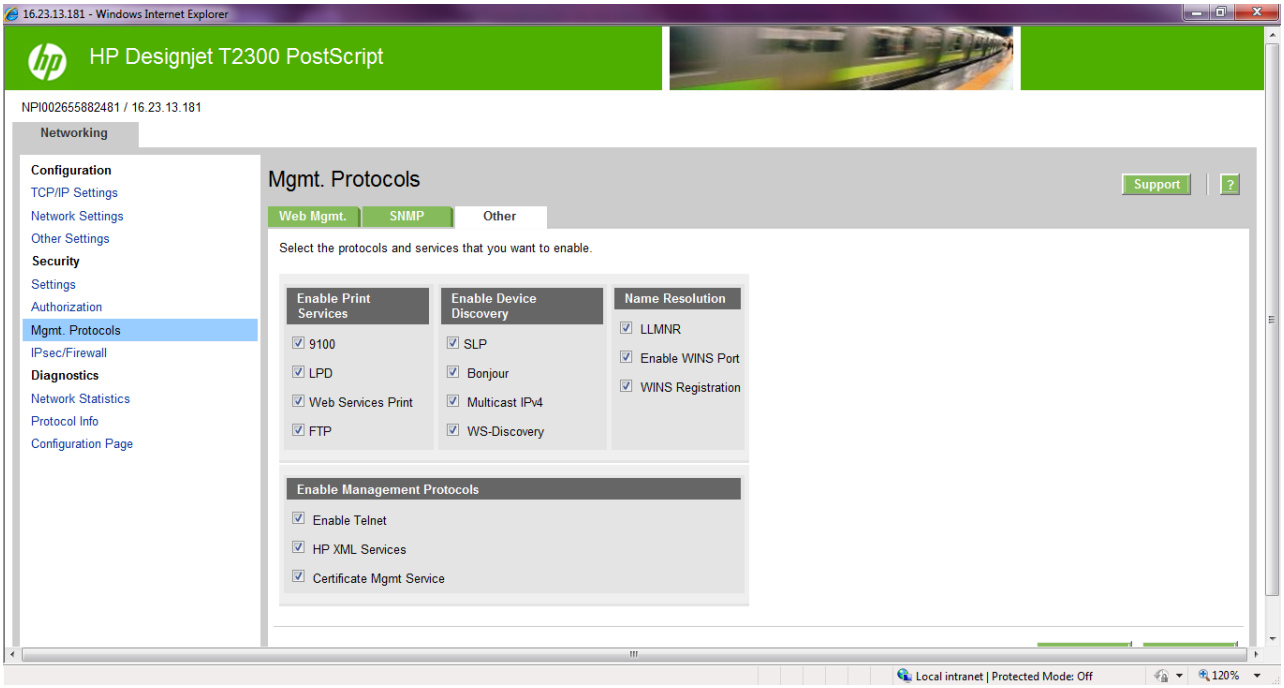


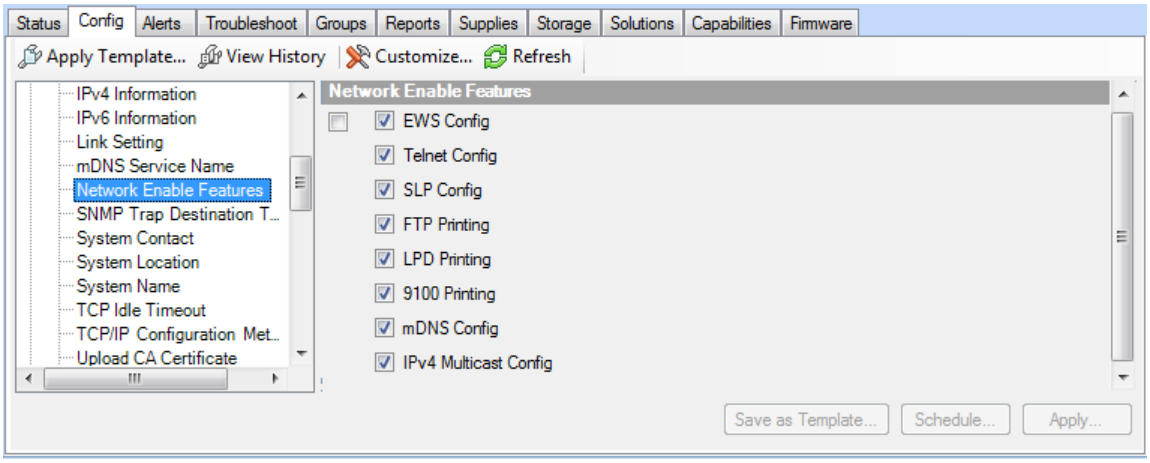
If you enable or disable a connectivity option, the printer will automatically restart. Keep in mind that disabling a connectivity option could cut off network access to the printer. As a security measure, you cannot disable the connection that you use to access the Embedded Web server.

Note: If the printer's front panel becomes locked and you are unable to unlock it, then you should contact HP support as soon as possible.

3.7 Disable protocols

In some cases you might want to disable all protocols that you do not plan to use to access your printer. For example, you might prevent users from sending files via ftp or connecting through telnet to manage the printer network settings. You can disable unused protocols through the Mgmt. Protocols option in the Embedded Web Server, or Network Enable Features in Web JetAdmin.





3.8 IPSec

A Firewall or IP Security (IPsec) policy enables you to control traffic to or from the device by using network-layer protocols. Either a firewall or IPsec / firewall pages will appear, depending on whether IPsec is supported by the print server and device. If IPsec is not supported, firewall pages will be displayed and a firewall policy can be configured.

Please note: Before you enable a firewall or IPsec policy, you should make sure that access to your configuration management settings is secured (for example, through an administrator password). This will ensure that your policy is not easily disabled through Telnet, control panel menus, or other management tools.

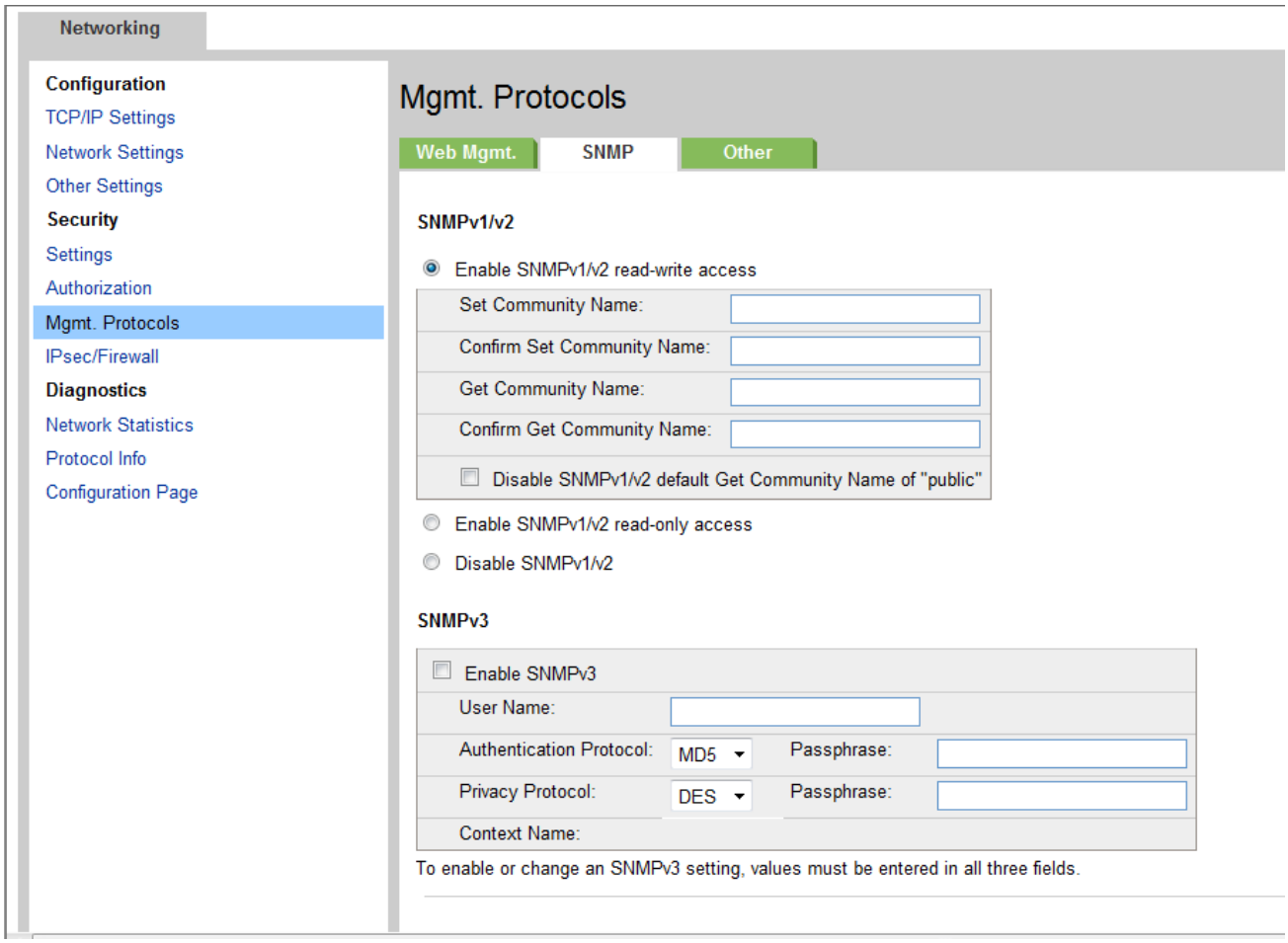
Firewall. Use this page to view or configure a firewall policy. A firewall policy consists of up to 10 rules, where each rule specifies the IP addresses and services that are allowed by the print server and device. To add a rule, click 'Add Rule'. This setting runs a wizard that will help you to configure each rule.

IPsec / Firewall. Use this page to view or configure an IPsec / firewall policy. An IPsec / firewall policy consists of up to 10 rules. As with a firewall policy, each rule specifies the IP addresses and services that are allowed by the print server and device. With IPsec support, you can apply IPsec authentication and encryption protocols for those addresses and services. To add a rule, click 'Add Rule'. This runs a wizard that will help you to configure each rule.

For a detailed description of wizard settings and additional help, visit **Jetdirect IPsec/Firewall Help**.

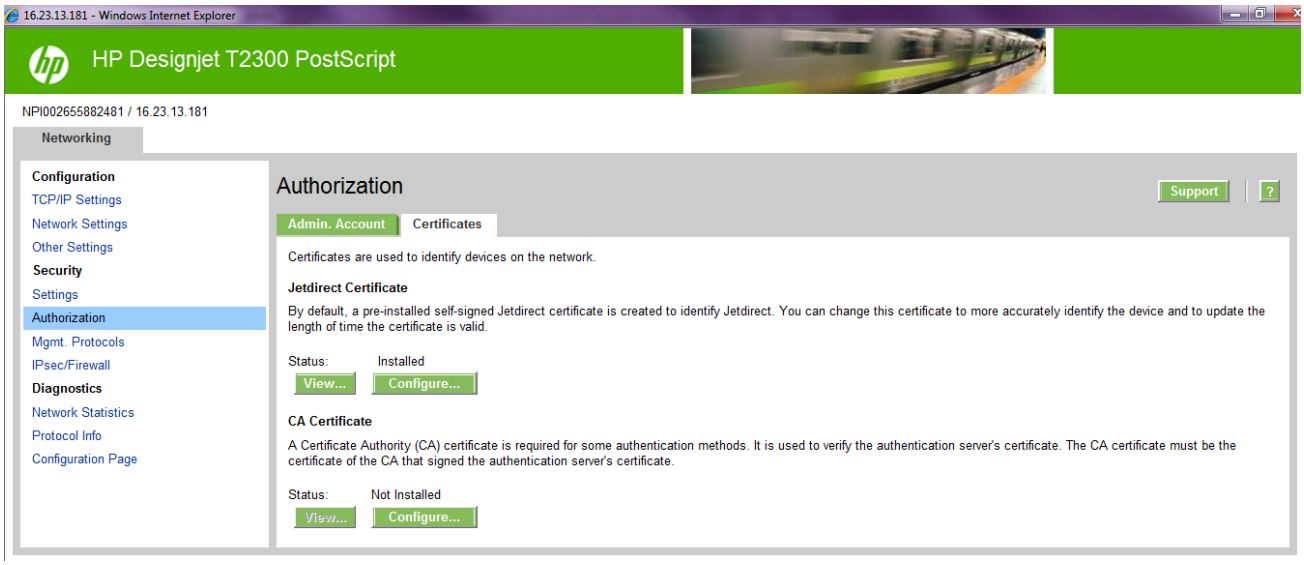
3.9 SNMPv3

You can enable and disable the SNMP v3 agent from your printer. You may set up an account that allows a management application to access the SNMP v3 agent.



3.10 CA/JD Certificates

You can request, install, and manage digital certificates on the HP JetDirect print server. Certificates are used to identify the JetDirect print server both as a valid Web server for network clients, and as a valid client requesting access on a secure network. By default, the JetDirect print server contains a self-signed, pre-installed certificate.



3.11 Hide IP from front panel

Some printers include an option in the Service Menu, accessible with the help of an HP Support agent only, that enables you to hide all IP information from the printer's front panel.

3.12 Encrypt web communications

You can securely manage your network-connected printers using a Web browser and the HTTPS protocol. To authenticate the HP JetDirect Web Server when HTTPS is used, you may configure a certificate, or you may use the pre-installed, self-signed X.509 Certificate. The encryption strength specifies what ciphers the web server will use for secure communications. Supported cipher suites are DES, RC4, and 3DES.

When you enable encryption, the web server encrypts all web communication, forcing all connections to use HTTPS. You can also configure encryption options to allow both HTTP (unencrypted) and HTTPS connections. In secure environments, you should choose to encrypt all web communications. Otherwise, sensitive management data (Administrator Password, SNMP Community Names, and secret keys) may be compromised.

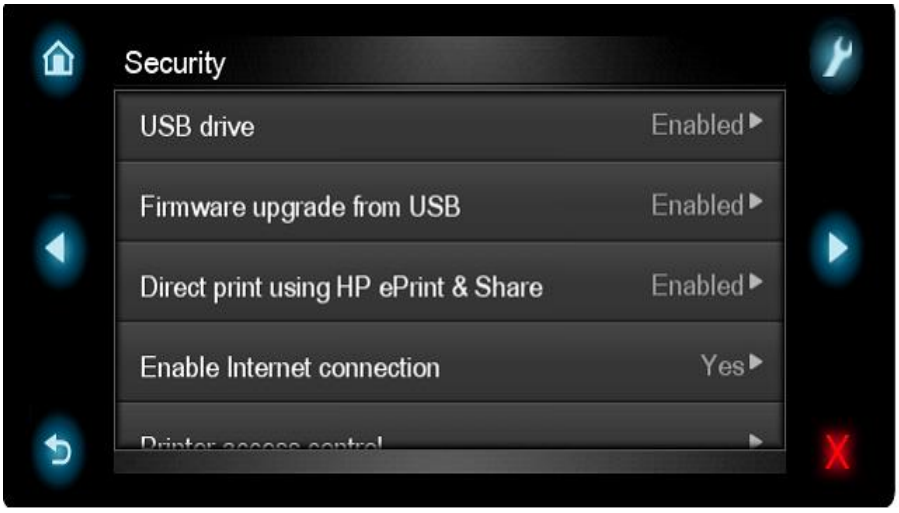
OpenSSL HeartBleed Vulnerability

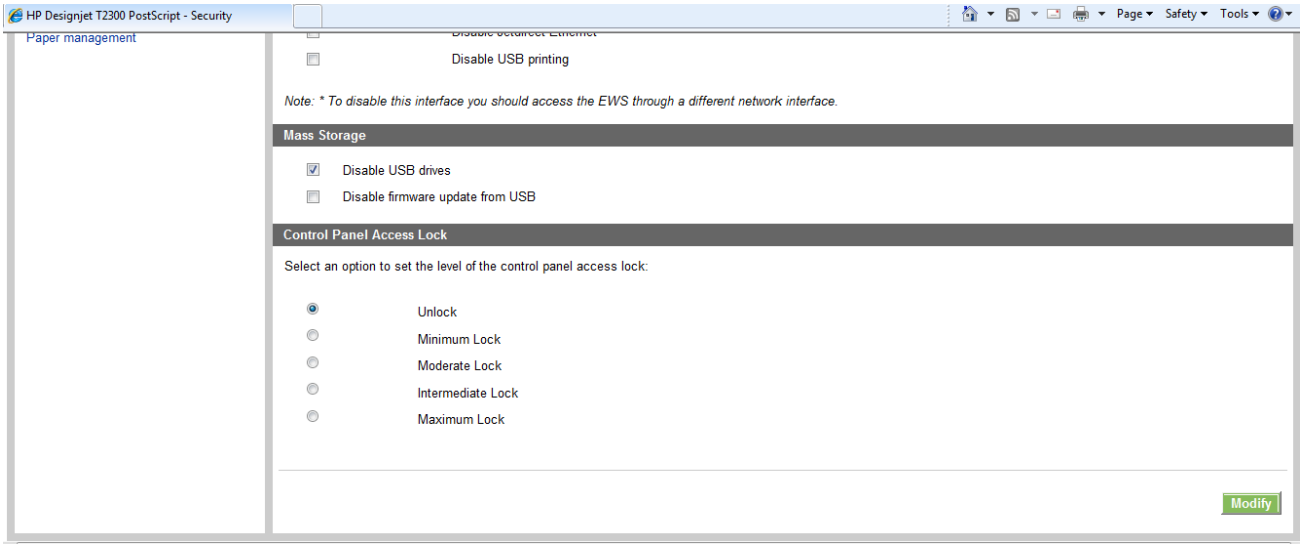
On April 8, 2014 HP Networking support was notified of the vulnerability known as Heartbleed in the open-source and widely-used OpenSSL toolkit. The vulnerability allows unauthenticated access to portions of computer system memory.

HP Designjet products are not vulnerable due to either using a version of OpenSSL that is not vulnerable or are not using protocol objects affected.

3.13 Disable USB drive

You can use this option to disable the use of USB drives, preventing somebody from connecting a device to print or to scan images.





3.14 Disable firmware update through USB

This option is used to disable the possibility of upgrading the printer by installing new firmware from a USB device.

3.15 Disable direct print using ePrint&Share

Some printers have a feature that enables you to connect a computer directly with a USB cable, and then print without installing any driver. This can be done by launching the ePrint&Share application that is pre-installed on the printer. It is possible to disable this feature, however, so that you cannot print via the USB unless you have the driver (or ePrint&Share) installed on the connected computer.

3.16 Disable ePrint Center connectivity

This feature disables the ePrint Center functionality so that users are unable to remotely send items to print.

3.17 User sessions

This feature enables you to set a timeout so that open sessions to ePrint&Share from the printer front panel are automatically closed if they are not used within the set time.

3.18 Disable internet connection

Disable the direct connection of the printer to the internet. This option also prevents the printer from automatically performing firmware upgrades.

3.19 Printer Access control

For some printers, when setting an Embedded Web Server Admin password, you also restrict access to certain front panel features. The protected features on the front panel are:

- Network connectivity & Internet connectivity
- Control firmware upgrades
- Reset factory defaults
- External hard disk connection
- Security

If a user loses the admin password, it is not possible to reset it and the printer will be locked. There is a service menu option to reset the admin password. Only customer service agents can do this.

3.20 External hard disk (EHD)

Some printers allow the connection of an external hard disk. Any HP Designjet printer with an internal hard disk uses it for four main purposes:

- Storing the printer's firmware & resources (media profiles, demo plots, diagnostic plots).
- Providing virtual memory for job processing.
- Storing/queuing jobs
- Storing the printer's accounting data.

The HP Designjet External Hard Disk was designed for a specific purpose, however. It enables security conscious customers to preserve the confidentiality of the jobs being printed on their HP Designjet printers.

3.20.1 How the system works

1. Connect the External Hard Disk (EHD) to the printer's USB host port.
2. The printer will detect the EHD and will ask for permission to install it. When you accept, the printer will move onto the next step.
3. All of the information normally stored on the internal HD is copied to the external HD.
4. Your printer's internal HD partition is then deleted using a highly secure erasing process (**DoD 5220.22-M**).
5. The printer is configured to use the EHD as the repository for ALL future jobs (including the temporary processing storage area).
6. When the printer is switched off, as a security measure, the EHD can be removed and kept in a secure location.

Notes:

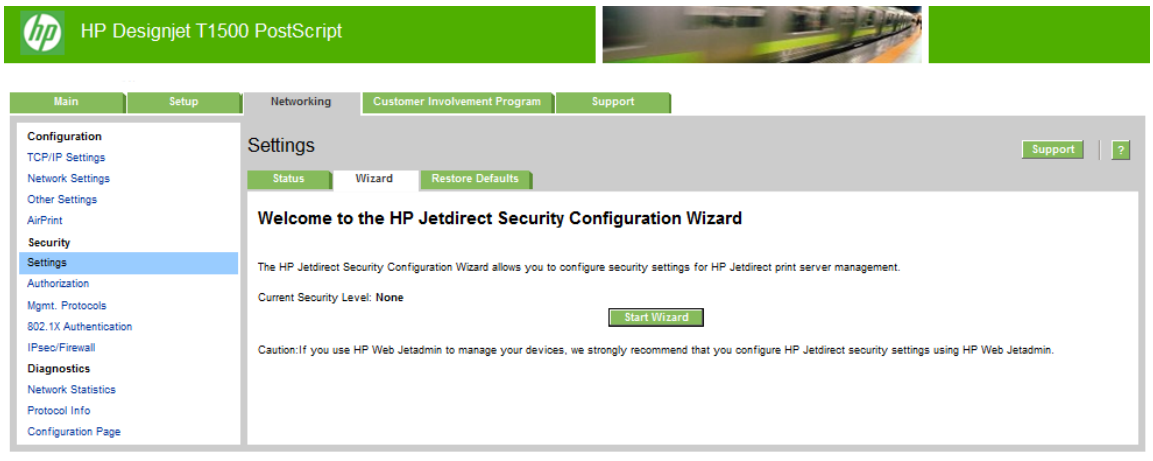
- Once the printer has an EHD installed it can no longer be initialized without it.
- If for any reason the installed EHD is no longer available (if you should lose the EHD, or the EHD is broken), there is a mechanism (through a special bootmode controlled with a specific front panel key combination) that reconfigures the printer to work without the EHD. However in that particular case, all the information stored on the EHD is lost.
- Once the EHD is installed on a particular printer, it becomes fully tied to it. It is not possible to move the same EHD to another HP Designjet printer without losing the stored information. When the printer detects an EHD that has been installed on a different printer, it will display a warning. If you then decide to go ahead and use the EHD on a different printer, the printer will erase the contents of the EHD (once again, using the highly secure **DoD 5220.22-M** process)
- The EHD has its own software-based encryption mechanism that prevents anyone from reading the contents of the EHD, for instance, by plugging it into a PC. The encryption system is not a standard system, and cannot be considered as an extremely secure encryption mechanism (such as the standard encryption system **DES**, **RSA**, **FIPS 140**), but it does add a level of security that makes it difficult to read the contents by simply connecting the disk to a PC.

The EHD is not intended to be used as an USB memory stick, that is, to copy documents from a PC, then plug it into the printer in order to print them.

3.21 Jetdirect Security Wizard (HP T920-T1500-T2500-T3500)

The HP Jetdirect Security Configuration Wizard enables you to configure security settings for HP Jetdirect print server management. There are 3 levels of Network Security that can be set:

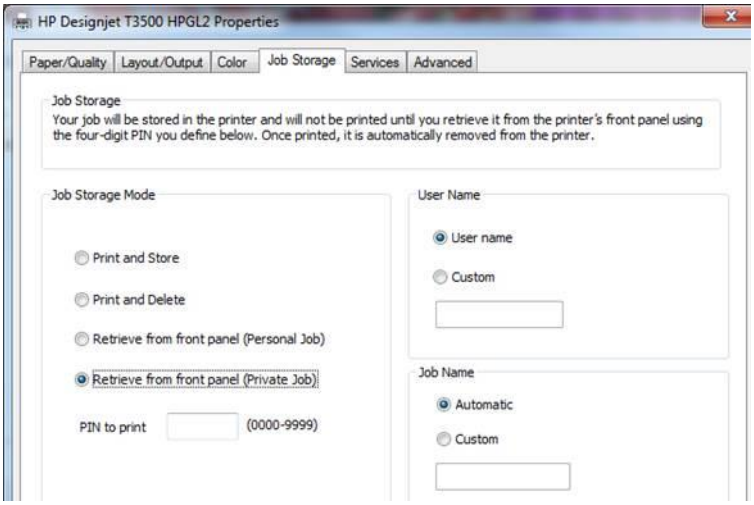
Basic	Configure an Admin password which is shared on other tools such as Telnet and SNMPv1/v2.
Enhanced	Disable unsecure management protocols (FTP, Telnet, RCFG, SNMP v1/v2c). Enable SNMPv3. Enable SNMPv1/v2 read only access.
Custom	Manually adjust all the settings.



3.22 Job storage and PIN printing

Job storage allows jobs to be stored and then printed when required, it also provides features for setting print jobs as “private”, with a personal identification number (PIN).

To access job storage features, open the printer Properties, and then select Printing Preferences. Click on the Job Storage tab where the following job-storage features are available:



Print and Store:

- After a job has printed, it is stored in the printer, more copies can then be printed from the front panel.

Print and Delete:

- Once printed, the job is automatically removed from the printer.

Retrieve from Front Panel (Personal Job):

- Use the personal job printing feature to specify a job cannot be printed until you release it from the printer's front panel.

- To preview it in the Embedded Web Server you will need to enter the PIN.

Retrieve from Front Panel (Private Job):

- Use the private printing feature to specify that a job cannot be printed until you release it with a PIN. First, select "Retrieve from Front Panel (Private Job) and then the "Pin to Print" checkbox will be available. If checked, a 4-digit personal identification number must be set. The PIN is sent to the device as part of the print job. After sending the print job to the device, use the PIN to print the job. Once printed, it is automatically removed from the printer.

- To preview it in the Embedded Web Server in the Front Panel you will need to enter the PIN.

Note
Some Multifunction devices include Scan Job storage that has two options: Scan and delete (job is not stored in the scan job queue) and Scan and store (the job is kept in the scan job queue).

3.23 Self Encrypted hard disk

The Self Encrypted hard disk ensures data is automatically encrypted every time data is sent to the printer and is written to the drive. This is achieved using AES 256-bit and FIPS 140 encryption that ensure that data can't be read or extracted from the HDD.

Hard disk is protected also with an ATA password that is unique for each printer and changeable when required using EWS setup tab. This feature allows customers to update HDD password based on their IT security policy periodically.

5. Other security features available only through JetDirect

Some security features are available only after installing a JetDirect 640n or similar internal print server.

4.1 Access Control list

This feature lets you determine the access control list (ACL), which is used to specify the IP addresses on your network that are allowed access to the device. The ACL is normally used for security purposes and supports up to 10 entries. The device blocks communications from all other addresses. If the list is empty, any system is allowed access. By default, host systems with HTTP connections (such as web browser or IPP connections) are allowed access regardless of ACL entries. This allows hosts to access the device when proxy servers or Network Address Translators (NATs) are used. However, unfiltered access by HTTP hosts may be disabled by clearing the Check ACL for HTTP checkbox.

Host systems that have access are specified by their IP host or network address. If the network contains subnets, an address mask may be used to specify whether the IP address entry is for an individual host system or a group of host systems. For an individual host system, the mask “255.255.255.255” is assumed and is not required.

CAUTION! You may lose your ability to communicate with the device if your system is not properly specified in the list, or access through HTTP is disabled. If communication with the device is lost, then it may be necessary to restore the network settings to their factory-default values.

4.2 802.1X Authentication

802.1X is an IEEE Standard for port-based Network Access Control. It provides an authentication mechanism for devices that want to connect to a LAN.

For most 802.1X networks, the infrastructure components (such as LAN switches) must use 802.1X protocols to control a port's access to the network. If these ports do not allow partial or guest access, then the print server may need to be configured with your 802.1X parameters prior to connection.

To configure initial 802.1X settings before connecting to your network, you can use an isolated LAN, or a direct computer connection via a cross-over cable.

The supported 802.1X authentication protocols and associated configuration depend on the print server model and firmware version. For more information on 802.1X features please visit **here**.

6. Glossary

Active Directory (AD)	An advanced, hierarchical directory service that comes with Microsoft Windows servers (version 2000 or later). It is LDAP-compliant and built on the domain naming system (DNS) used on the Internet. Workgroups are given domain names, exactly like Web sites, and any LDAP-compliant client – such as Windows, Mac, or Unix – can gain access.
Adobe PostScript	Developed by Adobe, this is the standard page description language (PDL) for the graphics arts industry and commercial printing. Many printing devices support PostScript with a built-in PostScript interpreter
Color Access Control	Settings to determine which users and/or applications are allowed to print in color
Device Password (LJ feature)	This is equivalent to the designjet's web server password. It helps protect the printer from unauthorized access through remote applications
Domain Naming System (DNS)	Converts host names and domain names into IP addresses on the internet or on local networks that use the TCP/IP protocol.
Embedded Web Server (EWS)	The EWS resides on a hardware device (such as an HP Designjet) or in the printer firmware. The EWS enables you to review, configure, and change settings on an HP Designjet after inputting an IP address into a Web browser from your computer
File System Access settings (LJ feature)	File system access settings: The File System Access options enable you to completely disable many of the access points to the printer's data storage system. These access points are for various types of usage for the printer. The options are: • PJL disk access • SNMP disk access • NFS disk access • PS disk access HP recommends enabling PS Disk Access to allow you to print PS files, and disabling the rest
File System Password (LJ feature)	The File System Password feature helps protect the printer's data storage system options from unauthorized access. With the File System password configured, the printer requires the password before it will allow configuration changes to features that affect the data storage system. Some of these features are the Secure disk erase mode, the Secure Storage Erase feature, and the File System Access options.
Hide IP address from front Panel	An option in the Service Utilities menu of the front panel to show/hide the Internet Protocol (IP) address of your printer. If the address is hidden, only registered users or network administrators will know the correct address to submit jobs to the printer

HP Web Jetadmin	A web-based fleet management software tool for remote installation, configuration, problem resolution, proactive management, and reporting. For more information go to; **www.hp.com/go/webjetadmin**
IP multicast	A one-to-many transmission of data over an IP network.
IPSec	Internet Protocol Security (IPsec) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. In our case, IPsec is used to protect data flows between the host and the printer.
Job Held Timeout (LJ feature)	This feature is part of the Job Retention feature. It limits a held job to the selected time, and then the printer deletes it. You should select a reasonable timeout value for this setting to allow enough time for a user to walk to the printer to print a job or to allow time for jobs to print in a queue.
Job Retention (LJ feature)	This feature provides job retention options such as private job and hold job. You will be able to ensure that they are present during printing to provide privacy for documents in the printer output bins.
Multicast DNS (mDNS)	Also known as Bonjour or Rendezvous, mDNS uses IP multicast with DNS to provide the capabilities of a DNS server for service discovery in a small network that does not have a DNS server.
NTLM	NTLM is a suite of authentication and session security protocols used in various Microsoft network protocol implementations. There are two types of authentications named NTLMv1 and NTLMv2, version 2 improves security authenticaion over version 1.
PJL Password (LJ feature)	The PJL password feature helps to protect the printer from unauthorized configuration changes through Print Job Language (PJL) commands. It does not affect ordinary print jobs. Once the PJL password is configured, the MFP requires it before it will process any of these commands
Remote Firmware Upgrade (LJ feature)	This service allows an administrator to use a custom application to upgrade the printer's firmware remotely. Since HP recommends using HP Web Jetadmin to upgrade MFP firmware, you should disable Remote Firmware Upgrade.
Simple Network Management Protocol (SNMP)	This is a network monitoring and control protocol.
SNMPv3	SNMP (Simple Network Management protocol) allows users to manage the printer by using SNMP management tools, such as HP Web JetAdmin. SNMP is also the protocol for communicating from the printer to the Windows driver. SNMPv3 provides security through user authentication and data encryption
Subnet	A logical division of a local area network, which is created to improve performance and provide security. A subnet limits the number of nodes that compete for bandwidth.

Authentication Manager (LJ feature)	This feature enables administrators to secure Device Functions by requiring users to log in with a specific Log In Method for each Function. For example, users may be required to log in with an Access Code or PIN to make copies, yet be required to log in with a username and password to send e-mails. Log In Methods: The following Log In Methods are available with the latest device firmware upgrade: Group 1 PIN: Requires users to input a numeric code for access when at the control panel of the device. The numeric code entered by the walk-up user is compared to the first of two PINs stored on the device by the Administrator. When the PIN is entered correctly, the user can proceed. Group 2 PIN: Requires users to input a numeric code for access when at the control panel of the device. The numeric code is compared to the second of two PINs stored on the device by the Administrator. LDAP: Lightweight Directory Access Protocol, Requires users to input a username and password that are verified by an LDAP server. HP Digital Send Service (if available): Also known as DSS. Requires users to enter credentials that are verified by the HP Digital Send Service software. (HP Digital Send Service software must be available to use this Log In Method. If no DSS server is associated with this device, walk-up users will not be required to authenticate before using the device.) Kerberos: Requires users to enter a username and password to be verified by a Windows Server

For more information
About HP Designjet printers: **www.hp.com/go/designjet**
About HP WebJetAdmin: **www.hp.com/go/webjetadmin**

© 2014 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Adobe™ and PostScript™ are trademarks of Adobe Systems Incorporated, which may be registered in certain jurisdictions.

July 2014